Homogeneous Weights and Möbius Functions on Finite Rings *

Yun Fan, Hongwei Liu
Dept of Mathematics, Central China Normal University, Wuhan, 430079, China

Abstract

The homogeneous weights and the Möbius functions and Euler phi-functions on finite rings are discussed; some computational formulas for these functions on finite principal ideal rings are characterized; for the residue rings of integers, they are reduced to the classical number-theoretical Möbius functions and the classical number-theoretical Euler phi-functions.

Keywords: Finite ring, finite principal ideal ring, homogeneous weight, Möbius function, Euler phi-function.

2000 Mathematical Subject Classification: 94B05, 13A99.

1 Introduction

The homogeneous weight on finite rings is a generalization of the Hamming weight on finite fields and the Lee weight on the residue ring of integers modulo 4. Constantinescu and Heise [2] introduced the homogeneous weight on finite rings. Soon after, Greferath and Schmidt [6] proved the existence and uniqueness of the homogeneous weight on a finite ring, and exhibited a formula in terms of Möbius function and Euler phi-function to calculate the homogeneous weight, see Eqn (2.3) below for details. With the generating character, Honold [8] showed another formula to calculate the homogeneous weight on a finite Frobenius ring. In [13], with the help of the formula in [6], Voloch and Walker showed how to calculate the homogeneous weight on a finite Galois ring, and estimated the homogeneous weight of a algebraic geometry code. There are many related references, e.g. [1], [4], [3], [5].

However, it is not easy to obtain the values of the Möbius function and the Euler phi-function on a finite ring. In this paper we exhibit precise formulas to compute the Möbius function and the Euler phi-function on a finite principal ideal ring, which are similar to the classical results on the number-theoretical

*Supported by NSFC through Grant No. 10871079.
E-mail address: yunfan02@yahoo.com.cn (Yun Fan), h_w_liu@yahoo.com.cn (Hongwei Liu).

Möbius function and Euler phi-function; hence an explicit formula of the homogeneous weight on finite principal ideal rings is obtained. As an application, an explicit formula of the homogeneous weight on the residue rings of integers is formulated in terms of the classical number-theoretical Möbius function and Euler phi-function. In addition, we show a short proof of the result of [8] on the generating character and the homogeneous weight.

2 Homogeneous weights, Möbius functions and Euler phi-functions

In this section we make some preparations.

Let R be a finite ring with identity $1 \neq 0$; and $R^\times$ stand for the multiplication group consisting of all units (i.e. invertible elements) of R. For $x \in R$, set $Rx = \{rx \,|\, r \in R\}$ which is the left principal ideal of R generated by x. Let $\mathcal{P} = \{Rx \mid x \in R\}$ be the set of all left principal ideals of R. Obviously, $(\mathcal{P}, \supseteq)$ is a poset, where "$\supseteq$" is the inclusion relation. By $|X|$ we denote the cardinality of a set X. By $\mathbb{R}$ we denote the set of reals. The following is introduced in [2].

Definition 2.1. A map $w : R \to \mathbb{R}$ is called a *left homogeneous weight* if $w(0) = 0$ and the following two hold:

(H1) for $x, y \in R$, if $Rx = Ry$ then $w(x) = w(y)$;

(H2) there is a non-negative $\lambda \in \mathbb{R}$ such that for any non-zero $x \in R$ we have that $\sum\limits_{y \in Rx} w(y) = \lambda |Rx|$.

The condition (H2) implies that the average of the homogeneous weights on a non-zero left principal ideal is λ, which is independent of the choice of the left principal ideal.

Similarly, one can define *right homogeneous weights*, which coincide with left homogeneous weights once R is commutative. In the following, for convenience, the words "ideal" and "homogeneous weight" without further attributives stand for left ones.

For $x, y \in R$, if $rx = y$ for some $r \in R$ then we say that x divides y and denote it by $x|y$. If $x|y$ and $y|x$ (or equivalently, $Rx = Ry$), then we write $x \overset{g}{\sim} y$. Clearly, "$\overset{g}{\sim}$" is an equivalence relation on R, we call it the *association relation* on R; the equivalence class of the association relation is called the *association class*; cf. [9, p136]. By $\tilde{x}$ we denote the association class of x. Because R is a finite ring, one can check that $\tilde{x} = R^\times x = \{ux \mid u \in R^\times\}$. By definition, the association class $\tilde{x}$ is just the set of all the principal generators of the principal ideal Rx. Thus we make the following definition.

Definition 2.2. For $x \in R$, we set $\varphi(x) = |\tilde{x}| = \big|\{y \in R \mid Ry = Rx\}\big|$; and call $\varphi(x)$ the *Euler phi-function* on R.

Let $\mathcal{A} := \{\tilde{x} \mid x \in R\}$. If $x \,|\, y$, then for any $x' \in \tilde{x}$ and $y' \in \tilde{y}$ we have $x' \,|\, y'$; so we can write "$\tilde{x} \,|\, \tilde{y}$". Then ($\mathcal{A}$, "$\,|\,$") is a poset and

$$\mathcal{A} \xrightarrow{\cong} \mathcal{P}, \quad \tilde{x} \longmapsto Rx, \tag{2.1}$$

is an isomorphism of posets. Thus, Euler phi-function φ induces a function, denoted by φ again, defined on $\mathcal{P}$: for any $I \in \mathcal{P}$, $\varphi(I) = \varphi(x)$ where $x \in I$ such that $I = Rx$; in other words, $\varphi(I)$ is the number of the principal generators of the principal ideal I. Obviously, any ideal I of R is partitioned into disjoint union of association classes which are contained in I; by (2.1), any association class corresponds to exactly one principal ideal; so we have:

$$|I| = \sum_{J \in \mathcal{P},\, I \supseteq J} \varphi(J), \qquad \forall\, I \in \mathcal{P}.$$

According to the Möbius inversion on the poset $\mathcal{P}$ (see [9, §8.6]), we have

$$\varphi(I) = \sum_{J \in \mathcal{P},\, I \supseteq J} \mu(I,J) \cdot |J|, \qquad \forall\, I \in \mathcal{P}, \tag{2.2}$$

where $\mu(I,J)$ is the Möbius function on the poset $\mathcal{P}$ (hence on the poset $\mathcal{A}$).

Greferath and Schmidt [6] give the following formula: the homogeneous weight $w(x)$ of $x \in R$ is as follows

$$w(x) = \lambda \left(1 - \frac{\mu(Rx, 0)}{\varphi(x)} \right). \tag{2.3}$$

Remark 1. For later use, we sketch a short proof of the formula (2.3). The condition (H1) of Definition 2.1 says in fact that the homogeneous weight w is a function defined on $\mathcal{A} \cong \mathcal{P}$: for $I \in \mathcal{P}$ set $w(I) = w(x)$ with $x \in I$ such that $I = Rx$. Thus we can rewrite the condition (H2) of Definition 2.1 as follows:

$$\sum_{J \in \mathcal{P},\, I \supseteq J} \varphi(J) w(J) = \begin{cases} \lambda |I| & I \neq 0; \\ 0, & I = 0. \end{cases}$$

Define a function t on $\mathcal{P}$ as

$$t(I) = \begin{cases} \lambda |I|, & I \neq 0; \\ 0, & I = 0; \end{cases}$$

then

$$t(I) = \sum_{J \in \mathcal{P},\, I \supseteq J} \varphi(J) w(J). \qquad \forall\, I \in \mathcal{P}.$$

By the Möbius inversion on the poset $\mathcal{P}$, we have

$$\varphi(I) w(I) = \sum_{J \in \mathcal{P},\, I \supseteq J} \mu(I,J) t(J), \qquad \forall\, I \in \mathcal{P};$$

i.e.

$$w(I) = \frac{1}{\varphi(I)} \sum_{J\in\mathcal{P},\ I\supseteq J} \mu(I,J)t(J)\,, \qquad \forall\ I \in \mathcal{P}\,.$$

Observing the definition of the function $t(J)$, and noting that $|0| = 1$ where 0 stands for the zero ideal, by Eqn (2.2) we have the following computation:

$$\begin{aligned} w(I) &= \frac{1}{\varphi(I)} \sum_{0\neq J\in\mathcal{P},\ J\subseteq I} \mu(I,J)\cdot\lambda|J| = -\lambda\frac{\mu(I,0)}{\varphi(I)} + \frac{\lambda}{\varphi(I)} \sum_{J\in\mathcal{P},\ I\supseteq J} \mu(I,J)\cdot|J| \\ &= -\lambda\frac{\mu(I,0)}{\varphi(I)} + \frac{\lambda}{\varphi(I)}\cdot\varphi(I) = \lambda\left(1 - \frac{\mu(I,0)}{\varphi(I)}\right)\,; \end{aligned}$$

that is the formula (2.3).

3 Generating characters of finite Frobenius rings and Möbius functions

In this section we show a link between Möbius functions and generating characters on finite Frobenius rings, then deduce the Honold's formula for homogeneous weights in [8].

Recall that, for a finite additive group A, any homomorphism $\chi : A \to \mathbb{C}^\times$ is called a character of A, where $\mathbb{C}^\times$ is the multiplicative group of the complex field; at that case, the restriction $\chi|_B$ of χ to any subgroup B of A is of course a character of B, called the *restricted character* to B. The homomorphism mapping any $a \in A$ to $1 \in \mathbb{C}^timés$ is said to be the *unity character* and is denoted by 1.

For a finite ring R, any character of the additive group of the ring R is also called a character of the ring R. A character $\chi : R \to \mathbb{C}^\times$ is said to be a *generating character* if the restriction $\chi|_I$ to any non-zero principal ideal $I \in \mathcal{P}$ is not the unity character.

Wood [14] proved that a finite ring R is a Frobenius ring if and only if R has a generating character. We show that the Möbius function is related to generating characters.

Lemma 3.1. *Let R be a finite Frobenius ring and χ be a generating character of R. Then for any $x \in R$ we have:*

$$\mu(Rx, 0) = \sum_{y\in\widetilde{x}} \chi(y)\,. \tag{3.1}$$

Proof. We prove it by induction on the cardinality $|Rx|$. If $|Rx| = 1$, then $Rx = 0$ is the zero-ideal and $x = 0$, hence $\chi(0) = 1 = \mu(0,0)$. In the following we assume that $x \neq 0$ and set $I = Rx$. For $J \in \mathcal{P}$, we denote the set of principal generators of J by $\widetilde{J}$, i.e. $\widetilde{J} = \{y \in J \mid Ry = J\}$, which is just the

corresponding association class of J, see Eqn (2.1). Note that I is the disjoin union of association classes contained in I. So

$$\sum_{y\in I}\chi(y)=\sum_{J\in\mathcal{P},\,I\supseteq J}\;\sum_{y\in\widetilde{J}}\chi(y)=\sum_{y\in\widetilde{I}}\chi(y)+\sum_{J\in\mathcal{P},\,I\supsetneqq J}\;\sum_{y\in\widetilde{J}}\chi(y)\,.$$

Since the restriction $\chi|_I$ is a non-unity character of I, we get $\sum_{y\in I}\chi(y)=0$. By induction, for $J\in\mathcal{P}$ with $J\subsetneqq I$, we have $\sum_{y\in\tilde{J}}\chi(y)=\mu(J,0)$. Thus

$$\sum_{y\in\widetilde{I}}\chi(y)+\sum_{J\in\mathcal{P},\,I\supsetneqq J}\mu(J,0)=0\,.$$

On the other hand, as $I\neq 0$, in the partial order interval $[I,0]$ we have

$$\mu(I,0)+\sum_{J\in\mathcal{P},\,I\supsetneqq J}\mu(J,0)=\sum_{J\in\mathcal{P},\,I\supseteq J}\mu(J,0)=0\,.$$

Comparing the the above two equalities, we obtaine

$$\sum_{y\in\widetilde{I}}\chi(y)=\mu(I,0)\,.\quad\square$$

It follows at once from the above lemma and Eqn (2.3) that

Corollary 1. *Let R be a finite Frobenius ring, χ be a generating character of R, and w be the homogenous weight on R with average weight λ. Then for any $x\in R$ we have:*

$$w(x)=\lambda\left(1-\frac{1}{\varphi(x)}\sum_{y\in\widetilde{x}}\chi(y)\right)\,.\quad\square \tag{3.2}$$

We deduce Honold's formula in [8] from Eqn (3.2). Recall that the association class $\tilde{x}=R^\times x=\{ux\mid u\in R^\times\}$, i.e. the multiplicative group $R^\times$ acts by left translation on $\tilde{x}$ transitively. We denote the stable subgroup of x in $R^\times$ by $R^\times_x$. Then $\tilde{x}\cong R^\times/R^\times_x$. So

$$|R^\times|=|R^\times:R^\times_x|\cdot|R^\times_x|=|\tilde{x}|\cdot|R^\times_x|=\varphi(x)\cdot|R^\times_x|\,;$$

and

$$\sum_{u\in R^\times}\chi(ux)=\sum_{v\in R^\times/R^\times_x}\;\sum_{u\in vR^\times_x}\chi(ux)=\sum_{v\in R^\times/R^\times_x}|R^\times_x|\cdot\chi(vx)=|R^\times_x|\cdot\sum_{y\in\widetilde{x}}\chi(y)\,.$$

Substituting the above expressions into Eqn (3.2), we get

$$w(x)=\lambda\left(1-\frac{1}{|R^\times|}\sum_{u\in R^\times}\chi(ux)\right)\,,$$

which is just the formula for homogeneous weights in [8].

4 Möbius functions and Euler phi-functions on finite principal ideal rings

A finite ring is called a *chain ring* if all of its ideals form a chain with respect to inclusion relation. Let R be a finite chain ring. By definition, one can see that: R has a unique maximal ideal $\mathfrak{m}$, and the maximal ideal can be generated by one element γ, i.e. $\mathfrak{m} = R\gamma = \{\beta\gamma \mid \beta \in R\}$; there is a positive integer e, called the *nilpotent index* of R, such that $\gamma^e = 0$ but $\gamma^{e-1} \neq 0$; and

$$R = R\gamma^0 \supsetneqq R\gamma^1 \supsetneqq \cdots \supsetneqq R\gamma^{e-1} \supsetneqq R\gamma^e = 0$$

are all ideals of R. Let $\mathbb{F} = R/\mathfrak{m} = R/R\gamma$ be the residue field of R, with characteristic p, where p is a field. Then $|\mathbb{F}| = q = p^r$, $\mathbb{F}^\times = \mathbb{F} - \{0\}$ and $|\mathbb{F}^\times| = p^r - 1$. The following two lemmas are known, see [11].

Lemma 4.1. *Let notation be as above. For any $0 \neq r \in R$, there is a unique integer i, $0 \le i < e$ such that $r = u\gamma^i$, where $u \in R^\times$ is a unit, which is unique modulo γ^{e-i}.* □

Lemma 4.2. *Let notation be as above. Let $V \subseteq R$ be a set of representatives of R modulo $R\gamma$. Then*

(i) for any $r \in R$ there are unique $r_0, \cdots, r_{e-1} \in V$ such that $r = \sum_{i=0}^{e-1} r_i\gamma^i$;

(ii) $|V| = |\mathbb{F}|$;

(iii) $|R\gamma^j| = |\mathbb{F}|^{e-j}$ where $0 \le j \le e-1$. □

By Lemma 4.2, we have the cardinality of the chain ring R as follows.

$$|R| = |\mathbb{F}| \cdot |R\gamma| = |\mathbb{F}| \cdot |\mathbb{F}|^{e-1} = |\mathbb{F}|^e = q^e. \tag{4.1}$$

From now on we always assume that <u>R is a finite principal ideal ring</u>. Then we have finite chain rings $R_1, R_2, \cdots, R_s$ and an isomorphism of rings:

$$R \cong R_1 \times R_2 \times \cdots \times R_s. \tag{4.2}$$

Let $R_k\gamma_k$ for $k = 1, \cdots, s$ be the unique maximal ideal of R_k generated by γ_k with nilpotent index e_k, and $\mathbb{F}_{q_k} = R_k/R_k\gamma_k$ be the residue field of R_k with q_k elements, where q_k is a power of a prime p_k. Let $(\mathcal{P}_k, \subseteq)$ stand for the poset of all ideals of R_k which is a chain as follows:

$$R_k = R_k\gamma_k^0 \supsetneqq R_k\gamma_k^1 \supsetneqq \cdots \supsetneqq R_k\gamma_k^{e_k-1} \supsetneqq R_k\gamma_k^{e_k} = 0\,.$$

The integral interval $[0, e_k] = \{0, 1, \cdots, e_k - 1, e_k\}$ is also a chain: $0 \lneqq 1 \lneqq \cdots \lneqq e_{k-1} \lneqq e_k$; and the following map

$$[0, e_k] \longrightarrow \mathcal{P}_k\,, \quad i_k \longmapsto R_k\gamma_k^{i_k}\,, \tag{4.3}$$

is an anti-isomorphism of posets, i.e. the map is bijective and satisfies

$$i_k \le j_k \iff R_k\gamma_k^{i_k} \supseteq R_k\gamma_k^{j_k}\,.$$

For convenience, we denote

$$\mathcal{E} = [0, e_1] \times \cdots \times [0, e_s]\,,$$

which is the direct product of $[0, e_j]$ for $j = 1, \cdots, s$, i.e. $\mathbf{i} \in \mathcal{E}$ is written as $\mathbf{i} = (i_1, \cdots, i_s)$ with $i_k \in [0, e_k]$, and

$$\mathbf{i} \le \mathbf{j} \iff i_k \le j_k, \quad \forall\, k = 1, \cdots, s\,.$$

The ring isomorphism (4.2) induces an isomorphism of multiplicative groups:

$$R^\times \cong R_1^\times \times \cdots \times R_s^\times\,; \tag{4.2$^\times$}$$

for each k, $1 \le k \le s$, take $\rho_k \in R$ such that the image of ρ_k in $R_1 \times \cdots \times R_s$ is as follows

$$\rho_k \longmapsto (u_1, \cdots, u_{k-1}, \gamma_k, u_{k+1}, \cdots, u_s) \tag{4.4}$$

where $u_l \in R_l^\times$ provided $l \ne k$. By the isomorphisms (4.2) and (4.2$^\times$) we get the following lemma at once.

Lemma 4.3. *Notation as above. Each element x of R can be written as*

$$x = u\rho_1^{i_1}\cdots\rho_s^{i_s}\,, \qquad u \in R^\times, \quad (i_1, \cdots, i_s) \in \mathcal{E} = [0, e_1] \times \cdots \times [0, e_s]\,,$$

where $(i_1, \cdots, i_s)$ is uniquely determined by x. □

Let x be as in Lemma 4.3. Then the the image in $R_1 \times \cdots \times R_s$ of the ideal Rx of R is as follows:

$$Rx \longrightarrow R_1\gamma_1^{i_1} \times \cdots \times R_s\gamma_s^{i_s}\,. \tag{4.5}$$

So each ideal I of R is corresponding exactly to a unique $\mathbf{i} = (i_1, \cdots, i_s) \in \mathcal{E}$ such that

$$I = R \cdot (\rho_1^{i_1}\cdots\rho_s^{i_s})\,.$$

We denote the poset of principal ideals of R still by $\mathcal{P}$ as we did in §2; however, at the present case $\mathcal{P}$ is the set of all ideals of R because R is a principal ideal ring. Following the above discussion, we see that:

$$\mathcal{E} \longrightarrow \mathcal{P}, \quad \mathbf{i} \longmapsto R \cdot (\rho_1^{i_1}\cdots\rho_s^{i_s})\,.$$

is a bijection; and it is an anti-isomorphism of posets since (4.3) is an anti-isomorphism of posets.

For $\mathbf{i} = (i_1, \cdots, i_s) \in \mathcal{E}$, set $\bar{\mathbf{i}} = (\bar{i}_1, \cdots, \bar{i}_s) \in \mathcal{E}$ where $\bar{i}_k = e_k - i_k$, $k = 1, \cdots, s$. Then we obtain an anti-isomorphism of posets as follows:

$$\mathcal{E} \longrightarrow \mathcal{E}, \quad \mathbf{i} = (i_1, \cdots, i_s) \longmapsto \bar{\mathbf{i}} = (\bar{i}_1, \cdots, \bar{i}_s) = (e_1 - i_1, \cdots, e_s - i_s)\,. \tag{4.6}$$

Hence we obtain the following lemma.

Lemma 4.4. *Let notation be as above. The following is an isomorphism of posets:*

$$\mathcal{E} \longrightarrow \mathcal{P}, \quad \mathbf{i} \longmapsto R\cdot(\rho_1^{\bar{i}_1}\cdots\rho_s^{\bar{i}_s})\,. \qquad \square$$

Similarly to the classical Euler phi-function in the number theory, for q_k we define a q_k-phi-function as follows:

$$\varphi_k(q_k^{i_k}) = \begin{cases} q_k^{i_k} - q_k^{i_k-1}, & i_k > 0; \\ 1, & i_k = 0. \end{cases}$$

Further, we define a q-phi-function φ on $\mathcal{E}$ by:

$$\varphi(\mathbf{i}) = \prod_{k=1}^{s}\varphi_k(q_k^{i_k}) = \prod_{1\le k\le s,\, i_k>0}(q_k^{i_k} - q_k^{i_k-1})\,. \tag{4.7}$$

Let $x\in R$. By Definition 2.2, $\varphi(x)$ is just the cardinality of the association class $\tilde{x}$. By Lemma 4.3 and the anti-isomorphism (4.6), there is a unique $\mathbf{i} = (i_1,\cdots,i_s)\in\mathcal{E}$ such that $x = u\rho^{\bar{i}_1}\cdots\rho_s^{\bar{i}_s}$ with $u\in R^\times$.

Lemma 4.5. $\varphi(u\rho_1^{\bar{i}_1}\cdots\rho_s^{\bar{i}_s}) = \varphi(\mathbf{i}) = \prod_{1\le k\le s,\, i_k>0}\left(q_k^{i_k} - q_k^{i_k-1}\right)\,.$

Proof. By the correspondence (4.5), $\varphi(u\rho_1^{i_1}\cdots\rho_s^{i_s})$ is the number of the elements $x = (x_1,\cdots,x_s)$ such that $R_1x_1\times\cdots\times R_sx_s = R_1\gamma_1^{\bar{i}_1}\times\cdots\times R_s\gamma_s^{\bar{i}_s}$ (in the product of rings $R_1\times\cdots\times R_s$), equivalently, $R_kx_k = R_k\gamma_k^{\bar{i}_k}$ for all $k = 1,\cdots,s$. Since R_k is a chain ring, $R_kx_k = R_k\gamma_k^{\bar{i}_k}$ if and only if $x_k\in R_k\gamma_k^{\bar{i}_k} - R_k\gamma_k^{\bar{i}_k+1}$ (set difference). For $\bar{i}_k = e_k$ (equivalently, $i_k = 0$), it is obvious that $R_kx_k = R_k\gamma_k^{\bar{i}_k}$ if and only if $x_k = 0$. Thus

$$\varphi(u\rho_1^{\bar{i}_1}\cdots\rho_s^{\bar{i}_s}) = \prod_{1\le k\le s}\left|R_k\gamma_k^{\bar{i}_k} - R_k\gamma_k^{\bar{i}_k+1}\right| = \prod_{1\le k\le s,\, i_k>0}\left(q_k^{i_k} - q_k^{i_k-1}\right) = \varphi(\mathbf{i})\,.$$

$\square$

Recall that we denote the Möbius function on the poset $\mathcal{P}$ by $\mu(I,J)$ where $I,J\in\mathcal{P}$. We have the isomorphism of posets $\mathcal{P}\cong\mathcal{E} = [0,e_1]\times\cdots\times[0,e_s]$. For $\mathbf{i} = (i_1,\cdots,i_s)\in\mathcal{E}$ and $\mathbf{j} = (j_1,\cdots,j_s)\in\mathcal{E}$, we have the Möbius function $\mu(\mathbf{i},\mathbf{j})$. Since the Möbius function has product property (see [9, Theorem 8.10]), we have $\mu(\mathbf{i},\mathbf{j}) = \prod_{k=1}^{s}\mu_k(i_k,j_k)$, where $\mu_k(i,j)$ is the Möbius function on the poset $[0,e_k]$. Further, since $[0,e_k]$ is a chain, we have (see [9, Theorem 8.9]):

$$\mu_k(i_k,j_k) = \begin{cases} 1, & i_k - j_k = 0; \\ -1, & i_k - j_k = 1; \\ 0, & \text{otherwise.} \end{cases}$$

If there is an index k such that $i_k - j_k < 0$ or $i_k - j_k > 1$, then $\mu_k(i_k,j_k) = 0$ hence $\mu(\mathbf{i},\mathbf{j}) = 0$. Otherwise, $0\le i_k - j_k\le 1$ for all $k = 1,\cdots,s$; and $\mu_k(i_k,j_k)$

contributes $1, -1$ to $\mu(\mathbf{i}, \mathbf{j})$ when $i_k - j_k = 0, 1$ respectively. So

$$\mu(\mathbf{i}, \mathbf{j}) = \begin{cases} 0, & \text{if } i_k - j_k < 0 \text{ or } i_k - j_k > 1 \text{ for some index;} \\ (-1)^{\beta(\mathbf{i}, \mathbf{j})}, & \text{otherwise;} \end{cases} \tag{4.8}$$

where $\beta(\mathbf{i}, \mathbf{j}) = |\{k \mid i_k - j_k = 1\}|$, the number of indexes k such that $i_k - j_k = 1$.

Lemma 4.6. *Let $I, J \in \mathcal{P}$ correspond $\mathbf{i}, \mathbf{j} \in \mathcal{E}$, respectively, under the isomorphism in Lemma 4.4, i.e. $I = R \cdot (\rho_1^{\bar{i}_1} \cdots \rho_s^{\bar{i}_s})$, $J = R \cdot (\rho_1^{\bar{j}_1} \cdots \rho_s^{\bar{j}_s})$. Then*

$$\mu(I, J) = \mu(\mathbf{i}, \mathbf{j}) = \begin{cases} 0, & \text{if } i_k - j_k < 0 \text{ or } i_k - j_k > 1 \text{ for some index;} \\ (-1)^{\beta(\mathbf{i}, \mathbf{j})}, & \text{otherwise.} \end{cases}$$

where $\beta(\mathbf{i}, \mathbf{j})$ is the number of indexes k such that $i_k - j_k = 1$.

Proof. It follows from Lemma 4.4 and Eqn (4.8) immediately. $\square$

Noting that, by Lemma 4.3, any element of R is written as $u\rho_1^{\bar{i}_1} \cdots \rho_s^{\bar{i}_s}$ with $u \in R^\times$ and $\mathbf{i} = (i_1, \cdots, i_s) \in [0, e_1] \times \cdots \times [0, e_s]$, we get a precise formula to compute the homogeneous weight $w(-)$ on the finite principal ideal ring R as follows.

Theorem 4.1. *Let notation be as above. Then*

$$w\big(u\rho_1^{\bar{i}_1} \cdots \rho_s^{\bar{i}_s}\big) = \lambda \left(1 - \frac{\mu(\mathbf{i}, \mathbf{0})}{\varphi(\mathbf{i})}\right),$$

where $\mu(\mathbf{i}, \mathbf{0})$ is computed in Lemma 4.6 and $\varphi(\mathbf{i})$ is computed in Lemma 4.5. $\square$

As a special case where $s = 1$, we have the following corollary at once.

Corollary 2. *If R is a finite chain ring with a unique maximal ideal $R\gamma$ and nilpotent index e, then for any $x \in R$ we have*

$$w(x) = \begin{cases} 0, & x = 0; \\ \frac{\lambda q}{q-1}, & 0 \neq x \in R\gamma^{e-1}; \\ \lambda, & \textit{otherwise}; \end{cases} \qquad \textit{where} \quad q = |R/R\gamma|. \qquad \square$$

Proof. Write $x = u\gamma^{\bar{i}}$ with $u \in R^\times$ and $i \in [0, e]$, where $\bar{i} = e - i$. By Theorem 4.1 we have

$$w(x) = w(u\gamma^{\bar{i}}) = \lambda \left(1 - \frac{\mu(i, 0)}{\varphi(i)}\right).$$

If $x = 0$, i.e. $\bar{i} = e$ hence $i = 0$, then $\varphi(0) = 1 = \mu(0, 0)$; so $w(x) = 0$.

if $0 \neq x \in R\gamma^{e-1}$, i.e. $i = 1$, then, by Lemma 4.5, $\varphi(1) = q - 1$; by Lemma 4.6, $\mu(i, 0) = -1$; so

$$w(x) = \lambda \left(1 - \frac{-1}{q-1}\right) = \frac{\lambda q}{q-1}.$$

Otherwise, $e \geq i \geq 2$, then $\mu(i, 0) = 0$, hence $w(x) = \lambda(1 - 0) = \lambda$. $\square$

5 The homogeneous weight on the residue rings of integers

In this section we reformulate the computation of the homogeneous weight on the residue rings of integers with the classical Möbius function and the Euler phi-function in the number theory.

For any integer $m > 1$ we have a standard decomposition $m = p_1^{i_1} \cdots p_r^{i_r}$, where $p_1, \cdots, p_r$ are distinct primes and $i_k > 0$ for $k = 1, \cdots, r$. The classical number-theoretical Euler phi-function is:

$$\varphi(m) = \prod_{1 \le k \le r} \left(p_k^{i_k} - p_k^{i_k - 1}\right) ;$$

and the classical number-theoretical Möbius function is:

$$\mu(m) = \begin{cases} (-1)^r, & \text{if } i_k = 1 \text{ for all } k = 1, \cdots, r; \\ 0, & \text{otherwise.} \end{cases}$$

And $\varphi(1) = \mu(1) = 1$.

Theorem 5.1. *Let n be a positive integer, w be the homogeneous weight on $\mathbb{Z}_n$. Then any element of $\mathbb{Z}_n$ can written as $u \cdot n/m$ where $u \in \mathbb{Z}_n^\times$ and $m|n$, and*

$$w(u \cdot n/m) = w(n/m) = \lambda \left(1 - \frac{\mu(m)}{\varphi(m)}\right) .$$

Proof. Let $n = p_1^{e_1} \cdots p_s^{e_s}$ where $p_1, \cdots, p_s$ are distinct primes and $e_k > 0$ for all $k = 1, \cdots, s$. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}} ,$$

where $\mathbb{Z}_{p_k^{e_k}}$ is a chain ring with unique maximal ideal $p_k \mathbb{Z}_{p_k^{e_k}}$, nilpotent index e_k and residue filed isomorphic to $\mathbb{Z}_{p_k}$ of order p_k. The element $p_k \in \mathbb{Z}_n$ is mapped by the above isomorphism to:

$$p_k \longmapsto (p_k, \cdots, p_k, \cdots, p_k) ;$$

where the l'th coefficient p_k in the right hand size is a unit of $\mathbb{Z}_{p_l^{e_l}}$ provided $l \neq k$, compare with Eqn (4.4). Thus, by Lemma 4.3, any element a of $\mathbb{Z}_n$ is written as

$$x = u p_1^{l_1} \cdots p_s^{l_s}, \qquad u \in \mathbb{Z}_n^\times, \quad \mathbf{l} = (l_1, \cdots, l_s) \in \mathcal{E} = [0, e_1] \times \cdots \times [0, e_s].$$

Set $(i_1, \cdots, i_s) = \mathbf{i} = (e_1 - l_1, \cdots, e_s - l_s)$ and $m = p_1^{i_1} \cdots p_s^{i_s}$; then $x = u \cdot n/m$. So $w(x) = w(u \cdot n/m) = w(n/m)$, by Theorem 4.1, we have

$$w(n/m) = w(p_1^{\bar{i}_1} \cdots p_s^{\bar{i}_s}) = \lambda \left(1 - \frac{\mu(\mathbf{i}, \mathbf{0})}{\varphi(\mathbf{i})}\right) .$$

Further, by Eqn (4.7) we have

$$\varphi(\mathbf{i}) = \prod_{1\le k\le s,\, i_k>0} (p_k^{i_k} - p_k^{i_k-1}) = \varphi(m)\,;$$

and by Lemma 4.6 it is easy to check that $\mu(\mathbf{i},\mathbf{0}) = \mu(m)$. So

$$w(n/m) = \lambda\left(1 - \frac{\mu(m)}{\varphi(m)}\right). \qquad \square$$

Remark 2. More precisely, for $m = p_1^{i_1}\cdots p_s^{i_s}$ where $(i_1,\cdots,i_s) \in [0,e_1]\times\cdots\times[0,e_s]$, we have

$$w(n/m) = \begin{cases} \lambda, & \text{if there is an } i_k > 1;\\ \lambda(\varphi(m)-1)/\varphi(m), & \text{if every } i_k \le 1 \text{ and } \beta(m) \text{ is even};\\ \lambda(\varphi(m)+1)/\varphi(m), & \text{if every } i_k \le 1 \text{ and } \beta(m) \text{ is odd};\end{cases}$$

where $\beta(m)$ stands for the number k such that $i_k = 1$. In particular, for $m = n$ we get that

$$w(1) = \begin{cases} \lambda, & \text{if there is an } e_k > 1;\\ \lambda(\varphi(n)-(-1)^s)/\varphi(n), & \text{otherwise.}\end{cases}$$

Example 1. Applying Theorem 5.1, we calculate the Table 1 of the homogeneous weights on $\mathbb{Z}_{24}$, $\mathbb{Z}_{12}$ and $\mathbb{Z}_6$.

Table 1: Homogeneous weights on $\mathbb{Z}_{24}, \mathbb{Z}_{12}$ and $\mathbb{Z}_6$

$\mathbb{Z}_{24}$	$w(x)$	$\mathbb{Z}_{24}$	$w(x)$
0	0	12	2λ
1	λ	13	λ
2	λ	14	λ
3	λ	15	λ
4	$\frac{1}{2}\lambda$	16	$\frac{3}{2}\lambda$
5	λ	17	λ
6	λ	18	λ
7	λ	19	λ
8	$\frac{3}{2}\lambda$	20	$\frac{1}{2}\lambda$
9	λ	21	λ
10	λ	22	λ
11	λ	23	λ

$\mathbb{Z}_{12}$	$w(x)$
0	0
1	λ
2	$\frac{1}{2}\lambda$
3	λ
4	$\frac{3}{2}\lambda$
5	λ
6	2λ
7	λ
8	$\frac{3}{2}\lambda$
9	λ
10	$\frac{1}{2}\lambda$
11	λ

$\mathbb{Z}_6$	$w(x)$
0	0
1	$\frac{1}{2}\lambda$
2	$\frac{3}{2}\lambda$
3	2λ
4	$\frac{3}{2}\lambda$
5	$\frac{1}{2}\lambda$

Acknowledgements

The authors thank Prof Steven T. Dougherty for may helpful discussion.

References

[1] Byrne E., Greferath M., Honold T., *Ring geometries, two-weight codes, and strongly regular graphs*, Des. Codes, Crypt., Vol. 48, 1-16, 2008.

[2] Constantinescu I., Heise W., *A metric for codes over residue class rings of integers*, Problemy Peredachi Infromatsii, Vol. 33(3), 22-28, 1997.

[3] Greferath M., McGuire G. , O'Sullivan M. E., *Plotkin-Optimal Codes over Finite Frobenius Rings*, Journal of Algebra and its Applications, Vol. 5, 2006.

[4] Greferath M., O'Sullivan M. E., *On bounds for codes over Frobenius rings under homogeneous weights* , Discrete Mathematics, Vol. 289, 11-24, 2004.

[5] Greferath M., Schmidt S. E., *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory, Vol. 45, 2522-2524, 1999.

[6] Greferath M., Schmidt S. E., *Finite-ring combinatorics and Macwilliams' equivalence theorem*, J. Combin. Theory, Ser. A, Vol. 92, 17-28, 2000.

[7] Hammons A. R. , Jr., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P., *The Z_4 linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, Vol. 40, 301-319, 1994.

[8] Honold T., *Characterization of finite Frobenius rings*, Arch. Math. (Basel), Vol. 76(6), 406-415, 2001.

[9] Jacobson N., Basic Algebra I, second edition, W.H.Freeman and Company, 1985.

[10] MacWilliams F. J., Sloane N. J. A., *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[11] McDonald B. R., *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.

[12] Pless V. S., Huffman W. C., eds., *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998.

[13] Voloch J. F., Walker J. L., *Homogenous weights and exponential sums*, Finite Fields Appl., 310-321, 2003.

[14] Wood J., *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math., Vol. 121 (3), 555-575, 1999.